

FEDERAL BUREAU OF INVESTIGATION  
FOI/PA  
DELETED PAGE INFORMATION SHEET  
FOI/PA# 1204913-0

Total Deleted Page(s) = 32

Page 13 ~ b6; b7C; b7E;  
Page 14 ~ b7E;  
Page 15 ~ b7E;  
Page 16 ~ b6; b7C; b7E;  
Page 17 ~ b6; b7C; b7E;  
Page 18 ~ b7E;  
Page 19 ~ b7E;  
Page 25 ~ b6; b7C; b7E;  
Page 26 ~ b6; b7C; b7E;  
Page 27 ~ b6; b7C; b7E;  
Page 28 ~ b6; b7C; b7E;  
Page 29 ~ b6; b7C; b7E;  
Page 30 ~ b6; b7C; b7E;  
Page 31 ~ b6; b7C; b7E;  
Page 32 ~ b6; b7C; b7E;  
Page 33 ~ b6; b7C; b7E;  
Page 34 ~ b6; b7C; b7E;  
Page 35 ~ b6; b7C; b7E;  
Page 36 ~ b6; b7C; b7E;  
Page 37 ~ b6; b7C; b7E;  
Page 38 ~ b6; b7C; b7E;  
Page 39 ~ b6; b7C; b7E;  
Page 40 ~ b6; b7C; b7E;  
Page 41 ~ b6; b7C; b7E;  
Page 42 ~ b6; b7C; b7E;  
Page 44 ~ b6; b7C;  
Page 49 ~ b3; b6; b7C;  
Page 50 ~ b3; b6; b7C;  
Page 51 ~ b3; b6; b7C;  
Page 52 ~ b3; b6; b7C;  
Page 53 ~ b3; b6; b7C;  
Page 54 ~ b3; b6; b7C;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
X Deleted Page(s) X  
X No Duplication Fee X  
X For this Page X  
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

**Precedence:** ROUTINE

**Date:** 12/01/2011

**To:** San Diego

**From:** San Diego  
CY1

**Contact:** SA [REDACTED]

**Approved By:** [REDACTED]

**Drafted By:** [REDACTED]

**Case ID #:** 288A-SD-NEW (Pending)

**Title:** UNSUB(S);  
#ANTISEC;  
[REDACTED] - VICTIM;  
COMPUTER INTRUSION

**Synopsis:** Request case be opened on captioned investigation.

**Details:** On 11/18/2011, retired California Department of Justice Special Agent Supervisor [REDACTED] advised that he received text messages from his own Google telephone number indicating that he had been "owned".

On 11/18/2011, a YouTube video was posted with the title "#AntiSec Fuck FBI Friday V - Cybercrime Investigator Communications" from the YouTube user account [REDACTED]. The video was 6:03 long and stated the following information, which was also posted as text below the video:

"Greetings Pirates, and welcome to another exciting #FuckFBIFriday release.

As part of our ongoing effort to expose and humiliate our white hat enemies, we targeted a Special Agent Supervisor of the CA Department of Justice in charge of [REDACTED]. We are leaking over 38,000 private emails which contain detailed computer forensics techniques, investigation protocols as well as highly embarrassing personal information. We are confident these gifts will bring smiles to the faces of our black hat brothers and sisters (especially those who have been targeted by these scurvy dogs) while also making a mockery of "security professionals" who whore their "skills" to law enforcement to protect tyrannical corporativism and the status quo we aim to destroy.

UNCLASSIFIED

1A2

288A-SD-73148;1

UNCLASSIFIED

To: San Diego From: San Diego  
Re: 288A-SD-NEW, 12/01/2011

We hijacked two gmail accounts belonging to [redacted] who has been a cop for [redacted] years, dumping his private email correspondence as well as several dozen voicemails and SMS text message logs. While just yesterday [redacted] was having a private BBQ with his [redacted] high computer crime task force friends, we were reviewing their detailed internal operation plans and procedure documents. We also couldn't overlook the boatloads of embarrassing personal information about our cop friend [redacted] We lulzed as we listened to [redacted]

[redacted] We turned on his google web history and watched him [redacted]  
[redacted] We also abused his google voice account, making sure [redacted] friends and family knew how hard he was owned. Possibly the most interesting content in his emails are the [redacted]

[redacted] The information in these emails will prove essential to those who want to protect themselves from the techniques and procedures cyber crime investigators use to build cases. If you have ever been busted for computer crimes, you should check to see if your case is being discussed here. There are discussions about [redacted]

These cybercrime investigators are supposed to be the cream of the crop, but we reveal the totality of their ignorance of all matters related to computer security. For months, we have owned several dozen white hat and law enforcement targets-- getting in and out of whichever high profile government and corporate system we please and despite all the active FBI investigations and several billion dollars of funding, they have not been able to stop us or get anywhere near us. Even worse, they bust a few dozen people who are allegedly part of an "anonymous computer hacking conspiracy" but who have only used kindergarten-level [redacted] - this isn't even hacking, but a form of electronic civil disobedience.

We often hear these "professionals" preach about "full-disclosure," but we are sure these people are angrily sending out DMCA takedown notices and serving subpoenas as we speak. They call us criminals, script kiddies, and terrorists, but their entire livelihood depends on us, trying desperately to study our techniques and failing miserably at preventing future attacks. See we're cut from an entirely different kind of cloth. Corporate security professionals like Thomas Ryan and Aaron Barr think they're doing something noble by "leaking" the public email discussion lists of Occupy Wall Street and profiling the "leaders" of Anonymous. Wannabe player haters drop shitty dox and leak partial chat logs about other hackers, doing free work for law enforcement. Then you got people like Peiter "Mudge" Zatko who back in the day used to be old school l0pht/cDc only now to sell out to DARPA going around to hacker conventions encouraging others to work for the feds. Let this be a warning to aspiring white hat "hacker" sellouts and police collaborators: stay out the game or get owned and exposed. You want to keep mass arresting and brutalizing the 99%? We'll have to keep owning your boxes and torrenting your mail spools, plastering your personal information all over teh internets.

Hackers, join us and rise up against our common oppressors - the white hats, the 1%'s 'private' police, the corrupt banks and corporations and make 2011 the year of leaks and revolutions!

We are Anti-Security,  
We are the 99%  
We do not forgive.  
We do not forget.  
Expect Us!"

UNCLASSIFIED

b6  
b7C  
b7E

b7E

UNCLASSIFIED

To: San Diego From: San Diego  
Re: 288A-SD-NEW, 12/01/2011

A link was also provided on the YouTube page to the documents that were taken from [redacted] account. The information was located at [redacted]

Additionally, some of the information contained within [redacted] account was posted at [redacted]

b6  
b7C  
b7E

On 11/30/2011, California Department of Justice provided the FBI with a CD-ROM disc containing the files located at [redacted]. These files are contained in a 1-A envelope to this file and are password protected with the following password: [redacted].

♦♦

UNCLASSIFIED

UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

**Precedence:** ROUTINE

**Date:** 12/05/2011

**To:** San Diego

**From:** San Diego  
CY1

**Contact:** SA [REDACTED]

**Approved By:** [REDACTED] ✓

**Drafted By:** [REDACTED]

b6  
b7C

**Case ID #:** 288A-SD-73148 (Pending) , 2

**Title:** UNSUB(S);  
#ANTISEC;  
[REDACTED] VICTIM;  
COMPUTER INTRUSION

**Synopsis:** Document collection of [REDACTED] Gmail files from  
[REDACTED]

**Details:** On 12/01/2011, following a determination that the CD-ROM disc obtained from the California Department of Justice had become corrupted, SA [REDACTED] visited the website

b6  
b7C

[REDACTED] and downloaded the torrent containing the contents of the Gmail files exfiltrated from [REDACTED] accounts. The contents included one zipped file [REDACTED]

The zipped file was placed on a CD-ROM disc and placed in the 1-A file.

♦♦

UNCLASSIFIED

1A-1

288A-SD-73148; 2

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/07/2011

[redacted] date of birth [redacted] social security account number [redacted] was interviewed at the San Diego Division of the Federal Bureau of Investigation. Also attending the interview were ITCFE [redacted] and IA [redacted]. After being advised of the identity of the interviewing Agent and the nature of the interview, [redacted] volunteered the following information:

b6  
b7C

[redacted] referred to the written statement he had previously submitted and advised that the information provided within was accurate. A copy of the written statement is contained in a 1-A envelope in the file.

On 11/18/2011, at approximately 7:00 am PST, [redacted] began receiving text messages on his cellular telephone from the telephone number associated with his Google Voice account, [redacted]. The text messages were statements similar to "We have you" and "We own you". Additional text messages were received that directed [redacted] to enter an IRC chat room to discuss the matter with the individuals that had taken over [redacted] accounts. [redacted] advised that he did not reply to these messages and does not recall the exact context of the messages or the name of the IRC chat room that they were directing him to. [redacted] stated that he has deleted the text messages and has no record of them.

b6  
b7C

Shortly after receiving the text messages from the individuals claiming they had compromised his accounts, [redacted] began receiving telephone calls from friends and family members who advised him that they were receiving suspicious messages from him on Facebook. The individuals also advised that there were [redacted] and other out of character posts on his Facebook feed.

By noon [redacted] had recovered and locked down all of his accounts. Text messages continued arriving on his cellular telephone that appeared to be from his Google Voice telephone number. Fearing that his Google account was still compromised, [redacted] deleted the Google account.

b6  
b7C

Following the recovery of his accounts, [redacted] received a text message that stated that it wasn't over and a text message that made a reference to the tough economic times and financial

---

Investigation on 12/06/2011 at San Diego, CAFile # 288A-SD-73148 3 Date dictated \_\_\_\_\_by SA [redacted]b6  
b7C

288A-SD-73148

Continuation of FD-302 of [REDACTED]

, On 12/06/2011 , Page 2

issues. [REDACTED] checked his credit cards and discovered that a fraudulent charge had been made on his [REDACTED] card from Ritz camera. The item was set to ship to his old address. The [REDACTED] card that was used ended in [REDACTED]

b6  
b7C

[REDACTED] believed that the compromise could be related to his Android cellular telephone, which he had "rooted". One of the consequences of rooting the telephone was that other programs that normally would not have access to the files "Shared Preferences" and "Accounts.db" could now access those files. The files contain information such as [REDACTED] from the telephone. A few days prior to the individuals advising [REDACTED] that he had been compromised, [REDACTED] had downloaded and installed a program called "atorrent" from the Android store. This program allowed a user to download torrent files onto your cellular telephone. [REDACTED] stated that he used the program several times to test it, downloading music and a movie.

b6  
b7C

[REDACTED] also stated that his laptop could have been a potential source of the compromise, but did not believe that it could have been his desktop computer.

The password used for his Gmail account, [REDACTED]. The only other system that [REDACTED] All other passwords were [REDACTED]

b6  
b7C

Although #AntiSec claimed to compromise two Gmail accounts, [REDACTED] believed that the second account compromised may have been his Yahoo! account, [REDACTED] since he had to [REDACTED] stated that he was unsure how they would have determined that he was the owner of the Yahoo! account [REDACTED]

b6  
b7C

[REDACTED] was unaware if the Gmail account he had created for [REDACTED] had been compromised. Additionally, [REDACTED] did not remember the exact name of that account or the password for it.

[REDACTED] advised that he has wiped the hard drives of both his laptop and desktop computers. He also stated that he has deleted his Google account that was compromised and reset his

288A-SD-73148

Continuation of FD-302 of , On 12/06/2011, Page 3

b6  
b7c

Android cellular telephone  which removed all of the text messages he had received.



- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/05/2012

On 12/31/2011, an individual posted information regarding the compromise of the California State Law Enforcement Association (www.cslea.com) on www.pastebin.com. The information provided an explanation for the attack, e-mail communications from CSLEA personnel discussing the security of their website, as well as name, address, password, and credit card information for individuals related to CSLEA. Additionally, the message stated that the compromise of CSLEA was "how Special Agent [redacted] at the California DOJ [redacted] Unit got humiliated last month".

b6  
b7C

The referenced information has been printed out and attached to this document.

Investigation on 01/05/2012 at San Diego, CAFile # 288A-SD-73148 ; 5

Date dictated \_\_\_\_\_

by SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SD-73148; 5

PASTEBIN

Follow @pastebin

search...

CREATE NEW PASTE

TRENDING PASTES

SIGN UP LOGIN MY SETT

Untitled

BY: A GUEST | DEC 31ST, 2011 | SYNTAX: NONE | SIZE: 71.51 KB | HITS: 2,862 | EXPIRES: NEVER

COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

MY PASTES

PUBLIC PAS

Lou Reec

9 sec ago

Untitled

23 sec ago

Database

34 sec ago

inserting

54 sec ago

Untitled

1 min ago

Untitled

1 min ago

Untitled

2 min ago

Selecting

3 min ago

LAYOUT WI



```

1. Hello comrades and thanks for joining us for the final phase of our cross
2. country hacker crime spree, our contribution to pr0j3kt m4yh3m. We're still
3. preparing the torrents, mail spools, as well as our final txt zine release which
4. will surely bring humiliation and embarrassment to many white hats and
5. sysadmins. But this New Years Eve, we bringing yall some party favors to keep
6. you raging all night. Did you remember a month ago when the mayors and piggies
7. across the US conspired to attack protesters in public parks? We sure do, so we
8. have been planning a retaliatory raid of our own. Bring it, NDAA. Bring it,
9. SOPA. We are snipers with one hell of a scope! Takin out a cop or two, they
10. can't cope with us!
11.
12.                west coast - east coast
13.
14. /*****
15.    CALIFORNIA LAW ENFORCEMENT ASSOCIATION - DEFACED AND DESTROYED BY ANTISEC
16.    *****/
17.
18. Soundtrack to the Rev Track: The Coup - Five Million Ways to Kill a CEO
19.    http://www.youtube.com/watch?v=lJotps9V4as
20.
21.    I'm from the land where the Panthers grew
22.    You know the city and the avenue
23.    If you the boss we be smabbin through
24.    And we'll be grabbin' you
25.    To say "What's up with the revenue?"
26.
27. Most everybody already knows that we don't like police very much. Shit, just
28. about everybody hates them, everybody except for the rich and powerful who
29. depend on their protection. But which state got the most blood on their hands?
30. Well we already owned pigs in Texas and Arizona, and many many others; guess its
31. time to ride on the California police.
32.
33. From the murder of Oscar Grant, the repression of the occupation movement, the
34. assassination of George Jackson in San Quinten prison, the prosecution of our
35. anonymous comrades in San Jose, and the dehumanizing conditions in California
36. jails and prisons today, California police have a notorious history of brutality
37. and therefore have been on our hitlist for a good minute now.
38.
39. So we went ahead and owned the California State Law Enforcement Association
40. (CSLEA.COM), defacing their website and giving out live backdoors. We dumped a
41. few of their mail spools and forum databases, and we did get a few laughs out of
42. reading years of their private email correspondence (such as CSLEA's Legislative
43. and Police [redacted]
44. [redacted]. But what we were really after was their membership rosters, which

```

b6

b7C

SHARE PAS

4.8k

45. included the cleartext password of 2500 of their members, guaranteeing the  
46. ownage of many more California pigs to come.  
47.  
48. "But wait! Cops are people too! Part of the 99%!" orly? When these soulless  
49. traitors voluntarily chose to cross the picket line and side with the bosses and  
50. bureaucrats, they burned all bridges with working class. As the bootboys for  
51. capitalism they do not protect us, instead choosing to serve the interests and  
52. assets of the rich ruling class, the 1%. Many Occupiers are learning what many  
53. of us already know about the role of police in society when they violently  
54. attacked protesters occupying public parks. Now it's time to turn the table and  
55. start firing shots off in the right direction. Problem, officer?  
56.  
57. Interestingly, CSLEA members have discussed some of our previous hacks against  
58. police targets, raising concern for the security of their own systems. However  
59. [ ] deliberately made some rather amusing lies as to their security. He  
60. repeatedly denied having been hacked up until web hosts at [ ] showed him  
61. some of the backdoors and other evidence of having dumped their databases. We  
62. were reading their entire email exchange including when they realized that  
63. credit card and password information was stored in cleartext. This is about the  
64. time [ ] changed his email password, but not before receiving a copy of the  
65. 'shopper' table which contained all the CCs. Too late, [ ]  
66.  
67. In all fairness, they did make an effort to secure their systems after discovery  
68. of the breach. [ ]  
69. [ ]  
70. [ ]  
71. [ ]  
72. [ ]  
73. [ ]  
74.  
75. But we still had [ ] and were stealthily checking out the  
76. many other websites on the server, while also helping ourselves to thousands of  
77. police usernames and passwords (it's how Special Agent [ ] at the  
78. California DOJ [ ] Unit got humiliated last month). For two months, we  
79. passed around their private password list amongst our black hat comrades like it  
80. was a fat blunt of the dank shit, and now it's time to dump that shit for the  
81. world to use and abuse. Did you see that there were hundreds of @doj.ca.gov  
82. passwords? Happy new years!!  
83.  
84. /\*\*\*\*\*  
85. LIST OF SITES HOSTED BY CSLEA, NOW WIPED OFF THE NET !!!  
86. \*\*\*\*\*/  
87.  
88. Association of Conservation Employees (ACE)  
89. Association of Criminalists-DOJ (AC-DOJ)  
90. Association of Deputy Commissioners (ADC)  
91. Association of Motor Carrier Operations Specialists (AMCOS)  
92. Association of Motor Vehicle Investigators of California (AMVIC)  
93. Association of Special Agents-DOJ (ASA-DOJ)  
94. California Association of Criminal Investigators (CACI)  
95. California Association of Food and Drug Investigators (CAFDI)  
96. California Association of Fraud Investigators (CAFI)  
97. California Association of Regulatory Investigators and Inspectors (CARI)  
98. California Association of State Investigators (CASI)  
99. California Organization of Licensing Registration Examiners (COLRE)  
100. California Association of Law Enforcement Employees (CALEE)  
101. California Highway Patrol Public Safety Dispatchers Association (CHP-PSDA)  
102. Fire Marshal and Emergency Services Association (FMESA)  
103. Hospital Police Association of California (HPAC)

b6  
b7Cb6  
b7C  
b7Eb6  
b7D  
b7E

104. Resource Protection Peace Officers Association (RPPOA)  
105. State Employed Fire Fighters Association (SEFFA)  
106.  
107. /\*\*\*\*\*  
108. OUR FAVORITE SECTION IN ANY GOOD HACKING ZINE - EXPOSING THE CLUELESSNESS OF  
109. WHITE HAT SYSADMINS IN THEIR OWN WORDS. OUR STORY BEGINS IN AUGUST WHEN CSLEA  
110. TAKES NOTICES OF OUR PREVIOUS ATTACKS ON POLICE SYSTEMS. IS ANYONE SAFE?!  
111. \*\*\*\*\*/

112.  
113.  
114.  
115.  
116.  
117.  
118.  
119.  
120.  
121.  
122.  
123.  
124.  
125.  
126.  
127.  
128.  
129.  
130.  
131.  
132.  
133.  
134.  
135.  
136.  
137.  
138.  
139.  
140.  
141.  
142.  
143.  
144.  
145.  
146.  
147.  
148.  
149.  
150.  
151.  
152.  
153.  
154.  
155.  
156.  
157.  
158.  
159.  
160.  
161.  
162.

b6  
b7C

.225.  
.226.  
.227.  
.228.  
.229.  
.230.  
.231.  
.232.  
.233.  
.234.  
.235.  
.236.  
.237.  
.238.  
.239.  
.240.  
.241.  
.242.  
.243.

b6  
b7C  
b7E

.244. /\*\*\*\*\*  
.245. LOLOLOL SO MUCH FOR "ENCRYPTED MEMBER DATA". DAMN [REDACTED] YOU DID HALF THE WORK  
.246. FOR US. AND DESPITE BEING AWARE OF THE BREACH, YOU STILL COULD NOT KEEP US OUT.  
.247. ON TO THE NEXT TARGET.... NEW YORK POLICE CHIEFS, OWNED AND EXPOSED !!!  
.248. \*\*\*\*\*/

b6  
b7C

.250. Soundtrack to the Rev #3: Cop Killer by Ice-T

.251. <http://www.youtube.com/watch?v=p5gRIud57jQ>

.252.

.253. I got my black shirt on.

.254. I got my black gloves on.

.255. I got my ski mask on.

.256. This shit's been too long.

.257.

.258. I got my twelve gauge sawed off.

.259. I got my headlights turned off.

.260. I'm 'bout to bust some shots off.

.261. I'm 'bout to dust some cops off.

.262.

.263. I'm a cop killer, better you than me.

.264. Cop killer, fuck police brutality!

.265. Cop killer, I know your family's grieving, (fuck 'em!)

.266. Cop killer, but tonight we get even, ha ha.

.267.

.268. For our next owning we bring you multiple law enforcement targets in the state  
.269. of New York, who has been on our crosshairs for some time due to their brutal  
.270. repression of Occupy Wall Street. We also want to bring attention to the 1971  
.271. riots at Attica where in response to the murder of George Jackson, convicts took  
.272. over the prison, demanding humane living conditions. It is in this same spirit of  
.273. cross-country solidarity that we attacked police targets in NY.

.274.

.275. We're dropping the md5-hashed passwords and residential addresses for over 300  
.276. Police Chiefs in the state of New York. We are also sharing several private mail  
.277. spools of a few NY police chiefs. While most of the contents of these emails  
.278. involve boring day to day office work and blonde joke chain emails, there were  
.279. also treasure troves of embarrassing personal information as well as several  
.280. "For Official Use Only" and "Law Enforcement Sensitive" documents discussing  
.281. police methods to combat protesters.

.282.

.283. Subject: Mid Hudson Chiefs Fwd: Demonstrators

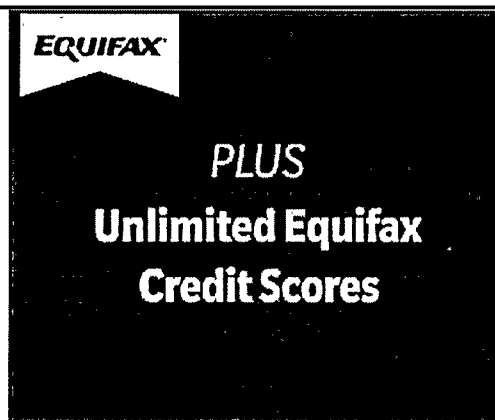
.343. [REDACTED]  
.344. [REDACTED]  
.345. [REDACTED]  
.346. There were also many parolee/probationers but the thought of betraying our  
.347. comrades under the gun of the prison industrial complex never crossed our minds.  
.348. But how about sum moar private police documents?? We dropped these on Bradley  
.349. Manning's birthday:  
.350. [REDACTED]  
.351. [REDACTED]  
.352. [REDACTED]  
.353. [REDACTED]  
.354. [REDACTED]  
.355. [REDACTED]  
.356. [REDACTED]  
.357. [REDACTED]  
.358. [REDACTED]  
.359. [REDACTED]  
.360. // THATS ALL FOR NOW KIDDIES! EXPECT A BADASS ZINE AND TORRENT COMING SOON!!!!!!

b6  
b7C  
b7E

RAW Paste Data

[CREATE NEW PASTE](#) | [CREATE NEW VERSION OF THIS PASTE](#)

b6  
b7C





PASTEBIN.COM TOOLS &amp; APPLICATIONS

[WINDOWS DESKTOP](#)[FIREFOX](#)[CHROME](#)[IPHONE & IPAD](#)[WEBOS](#)[ANDROID](#)[MAC](#)[OPERA](#)[CLIC](#)

1/5/12

Hello comrades and thanks for joining us for the final phase of our cross count - Pastebin.com

PASTEBIN.COM   CREATE NEW PASTE | API | TRENDS | USERS | FAQ | TOOLS | PRIVACY | CONTACT | ADVERTISE | STATS | GO PRO   
DOMAINS CENTER | PASTEBIN ON FACEBOOK | PASTEBIN ON TWITTER | PASTEBIN IN THE NEWS  
 OUR SITES: HOSTLOGR | TINYSUBS | URLSPY | FILESHUT | MORE... TIME: 0.01265

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/11/2012

[redacted] [redacted] provided  
a response to a Grand Jury Subpoena for [redacted]

[redacted] The following is a summary of the results of the  
subpoena:

b3  
b6  
b7C

The results have been printed out and are attached to  
this document for the file.

Investigation on 01/11/2012 at San Diego, CAFile # 288A-SD-73148

Date dictated \_\_\_\_\_

by SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency;  
it and its contents are not to be distributed outside your agency.

288A-SD-73148

v6



UNCLASSIFIED

**FEDERAL BUREAU OF INVESTIGATION**

**Precedence:** ROUTINE

**Date:** 01/26/2012

**To:** San Diego

**From:** San Diego  
CY1

**Contact:** SA [REDACTED]

**Approved By:** [REDACTED]

**Drafted By:** [REDACTED]

**Case ID #:** 288A-SD-73148 (Pending)

b6  
b7c

**Title:** UNSUB(S);  
#ANTISEC;  
[REDACTED] VICTIM;  
COMPUTER INTRUSION

**Synopsis:** Close captioned investigation.

**Details:** On November 18, 2011, retired California Department of Justice Special Agent Supervisor [REDACTED] advised that he received text messages from his own Google telephone number indicating that he had been "owned".

*[Handwritten mark]*

On November 18, 2011, a YouTube video was posted with the title "#AntiSec Fuck FBI Friday V - Cybercrime Investigator Communications" from the YouTube user account [REDACTED]. The video was 6:03 long and stated the following information, which was also posted as text below the video:

b6  
b7c

"Greetings Pirates, and welcome to another exciting #FuckFBIFriday release.

As part of our ongoing effort to expose and humiliate our white hat enemies, we targeted a Special Agent Supervisor of the CA Department of Justice in charge of [REDACTED]. We are leaking over 38,000 private emails which contain detailed computer forensics techniques, investigation protocols as well as highly embarrassing personal information. We are confident these gifts will bring smiles to the faces of our black hat brothers and sisters (especially those who have been targeted by these scurvy dogs) while also making a mockery of "security professionals" who whore their "skills" to law enforcement to protect tyrannical corporativism and the status quo we aim to destroy.

b6  
b7c

UNCLASSIFIED

288A-SD-73148; 7

1.27.12  
Close Case  
CS  
RB-1/27/12

UNCLASSIFIED

To: San Diego From: San Diego  
Re: 288A-SD-73148, 01/26/2012

We hijacked two gmail accounts belonging to [redacted] who has been a cop for [redacted] years, dumping his private email correspondence as well as several dozen voicemails and SMS text message logs. While just yesterday [redacted] was having a private BBQ with his [redacted] friends, we were reviewing their detailed internal operation plans and procedure documents. We also couldn't overlook the boatloads of embarrassing personal information about our cop friend [redacted] We lulzed as we listened to angry voicemails from [redacted]

[redacted] We turned on his google web history and watched him look up [redacted] [redacted] We also abused his google voice account, making sure [redacted] friends and family knew how hard he was owned. Possibly the most interesting content in his emails are the [redacted] internal email list archives (2005-2011) which [redacted]

b6  
b7C  
b7E

[redacted] The information in these emails will prove essential to those who want to protect themselves from the techniques and procedures cyber crime investigators use to build cases. If you have ever been busted for computer crimes, you should check to see if your case is being discussed here. There are discussions about [redacted]

[redacted]

These cybercrime investigators are supposed to be the cream of the crop, but we reveal the totality of their ignorance of all matters related to computer security. For months, we have owned several dozen white hat and law enforcement targets-- getting in and out of whichever high profile government and corporate system we please and despite all the active FBI investigations and several billion dollars of funding, they have not been able to stop us or get anywhere near us. Even worse, they bust a few dozen people who are allegedly part of an "anonymous computer hacking conspiracy" but who have only used kindergarten-level [redacted] this isn't even hacking, but a form of electronic civil disobedience.

b7E

We often hear these "professionals" preach about "full-disclosure," but we are sure these people are angrily sending out DMCA takedown notices and serving subpoenas as we speak. They call us criminals, script kiddies, and terrorists, but their entire livelihood depends on us, trying desperately to study our techniques and failing miserably at preventing future attacks. See we're cut from an entirely different kind of cloth. Corporate security professionals like Thomas Ryan and Aaron Barr think they're doing something noble by "leaking" the public email discussion lists of Occupy Wall Street and profiling the "leaders" of Anonymous. Wannabe player haters drop shitty dox and leak partial chat logs about other hackers, doing free work for law enforcement. Then you got people like Peiter "Mudge" Zatko who back in the day used to be old school l0pht/cDc only now to sell out to DARPA going around to hacker conventions encouraging others to work for the feds. Let this be a warning to aspiring white hat "hacker" sellouts and police collaborators: stay out the game or get owned and exposed. You want to keep mass arresting and brutalizing the 99%? We'll have to keep owning your boxes and torrenting your mail spools, plastering your personal information all over teh internets.

Hackers, join us and rise up against our common oppressors - the white hats, the 1%'s 'private' police, the corrupt banks and corporations and make 2011 the year of leaks and revolutions!

We are Anti-Security,  
We are the 99%  
We do not forgive.  
We do not forget.  
Expect Us!"

UNCLASSIFIED

UNCLASSIFIED

To: San Diego From: San Diego  
Re: 288A-SD-73148, 01/26/2012

A link was also provided on the YouTube page to the documents that were taken from [redacted] account. The information was located at [redacted]

b6  
b7C  
b7E

Additionally, some of the information contained within [redacted] account was posted at [redacted]

On November 30, 2011, California Department of Justice provided the FBI with a CD-ROM disc containing the files located at [redacted]. These files are contained in a 1-A envelope to this file and are password protected with the following password: [redacted]

On [redacted] responded to a Grand Jury subpoena issued in relation to [redacted]

b3  
b6  
b7C

Due to all victim information being destroyed and the lack of [redacted] [redacted] San Diego requests that captioned investigation be closed.

b3

♦♦

UNCLASSIFIED

- 1 -

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/26/2012

[redacted] e-mail address  
[redacted] was interviewed telephonically. After  
being advised of the identity of the interviewing Agent, [redacted]  
volunteered the following information:

[redacted]  
[redacted]

b3  
b6  
b7C

On 01/24/2012 [redacted] contacted the writer and advised  
that [redacted]

Investigation on 01/24/2012 at San Diego, CA (telephonically)

File # 288A-SD-73148 Date dictated \_\_\_\_\_

by SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

288A-SD-73148; 8